

Success
Successfully initiated launch of instance (i-0c9cefb7d66c1667)

▶ Launch log

Next Steps

Q. What would you like to do next with this instance, for example "create alarm" or "create backup"

< 1 2 3 4 5 6 >

Create billing and free tier usage alerts To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds. Create billing alerts	Connect to your instance Once your instance is running, log into it from your local computer. Connect to instance	Connect an RDS database Configure the connection between an EC2 instance and a database to allow traffic flow between them. Connect an RDS database	Create EBS snapshot policy Create a policy that automates the creation, retention, and deletion of EBS snapshots Create EBS snapshot policy
Manage detailed monitoring Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period. Manage detailed monitoring	Create Load Balancer Create a application, network gateway or classic Elastic Load Balancer Create Load Balancer	Create AWS budget AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location. Create AWS budget	Manage CloudWatch alarms Create or update Amazon CloudWatch alarms for the instance. Manage CloudWatch alarms

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Success
Successfully initiated launch of instance (i-0704b4e6fabe4b7ce)

▶ Launch log

Next Steps

Q. What would you like to do next with this instance, for example "create alarm" or "create backup"

< 1 2 3 4 5 6 >

Create billing and free tier usage alerts To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds. Create billing alerts	Connect to your instance Once your instance is running, log into it from your local computer. Connect to instance	Connect an RDS database Configure the connection between an EC2 instance and a database to allow traffic flow between them. Connect an RDS database	Create EBS snapshot policy Create a policy that automates the creation, retention, and deletion of EBS snapshots Create EBS snapshot policy
Manage detailed monitoring Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period. Manage detailed monitoring	Create Load Balancer Create a application, network gateway or classic Elastic Load Balancer Create Load Balancer	Create AWS budget AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location. Create AWS budget	Manage CloudWatch alarms Create or update Amazon CloudWatch alarms for the instance. Manage CloudWatch alarms

SMET Instance details | EC2 Manager

Successfully terminated i-0704b4e6fabe4b7ce

EC2 Instances i-0704b4e6fabe4b7ce

Instance summary for i-0704b4e6fabe4b7ce (WindowsServer) info

Updated less than a minute ago

Instance ID i-0704b4e6fabe4b7ce (WindowsServer)	Public IPv4 address 18.119.29.214 open address	Private IPv4 addresses 172.31.11.217
IPv6 address -	Instance state Shutting-down	Public IPv4 DNS ec2-18-119-29-214.us-east-2.compute.amazonaws.com open address
Hostname type IP name: ip-172-31-11-217.us-east-2.compute.internal	Private IP DNS name (IPv4 only) ip-172-31-11-217.us-east-2.compute.internal	Elastic IP addresses -
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address 18.119.29.214 [Public IP]	VPC ID vpc-07e91a4d1fc36a3cc	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-06e13760747a7a991	
IMD/Sv2 Optional		

Details Security Networking Storage Status checks Monitoring Tags

Instance details info

Platform windows
AMI ID ami-0b5f6cafef0c632bc
AMI name Windows_Server-2019-English-Full-Base-2023.03.15
Launch time Thu Apr 06 2023 09:40:06 GMT+0530 (India Standard Time) (9 minutes)

Monitoring disabled
Termination protection Disabled
AMI location amazon/Windows_Server-2019-English-Full-Base-2023.03.15

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

WindowServer.ipd EC-2.pem EC2.pem Show all

Screenshot of the AWS EC2 Management Console showing the instance details for i-0704b4e6fabe4b7ce (Windows Server). The instance was successfully terminated.

Instance summary for i-0704b4e6fabe4b7ce (WindowsServer) [Info](#)

Updated less than a minute ago

Instance ID	i-0704b4e6fabe4b7ce (WindowsServer)	Public IPv4 address	18.119.29.214 open address
IPv6 address	-	Instance state	Shutting-down
Hostname type	IP name: ip-172-31-11-217.us-east-2.compute.internal	Private IP DNS name (IPv4 only)	ip-172-31-11-217.us-east-2.compute.internal
Answer private resource DNS name	IPV4 (A)	Instance type	t2.micro
Auto-assigned IP address	18.119.29.214 [Public IP]	VPC ID	vpc-07e91a4d1fc36a5cc
IAM Role	-	Subnet ID	subnet-06e13760747a7a991
IMDSv2	Optional		

Details **Security** **Networking** **Storage** **Status checks** **Monitoring** **Tags**

Instance details: Info

Platform	AMI ID	Monitoring
Windows	ami-0b5f6c4fe0c632bc	disabled
Platform details	AMI name	Termination protection
Windows	Windows_Server-2019-English-Full-Base-2023.03.15	Disabled
Stop protection	Launch time	AMI location
Disabled	Thu Apr 06 2023 09:40:00 GMT+0530 (India Standard Time) (9 minutes)	amazon/Windows_Server-2019-English-Full-Base-2023.03.15

CloudShell **Feedback** **Language**

EC2 Management Console

Success Successfully initiated launch of instance i-0dfa272ea5366e169

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"?

- Create billing and free tier usage alerts
- Connect to your instance
- Connect an RDS database
- Create EBS snapshot policy
- Manage detailed monitoring
- Create Load Balancer
- Create AWS budget
- Manage CloudWatch alarms

CloudShell **Feedback** **Language**

aws Services Search [Alt+S]

EC2 > Instances > Launch an instance

Success Successfully initiated launch of instance (i-0a9b603873055f32e)

▶ Launch log

Next Steps

Q What would you like to do next with this instance, for example "create alarm" or "create backup"

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

[Create billing alerts](#)

Connect to your instance

Once your instance is running, log into it from your local computer.

[Connect to instance](#)

[Learn more](#)

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

[Connect an RDS database](#)

[Create a new RDS database](#) [Learn more](#)

Create EBS snapshot policy

Create a policy that automates the creation, retention, and deletion of EBS snapshots.

[Create EBS snapshot policy](#)

Manage detailed monitoring

Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.

[Manage detailed monitoring](#)

Create Load Balancer

Create an application, network gateway or classic Elastic Load Balancer

[Create Load Balancer](#)

Create AWS budget

AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.

[Create AWS budget](#)

Manage CloudWatch alarms

Create or update Amazon CloudWatch alarms for the instance.

[Manage CloudWatch alarms](#)

CloudShell Feedback Language [Alt+S]

New EC2 Experience Tell us what you think

Successfully created volume vol-0f8caa8e4b439146f

Volumes (2)

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Availability Zone	Volume state	Alarm status
-	vol-030a3aa75fbfb03b	gp2	30 GiB	100	-	snap-03d182c...	2023/04/06 10:21 GMT+5...	ap-southeast-1a	In-use	No alarms
-	vol-0f8caa8e4b439146f	gp2	5 GiB	100	-	-	2023/04/06 11:13 GMT+5...	ap-southeast-1a	Creating	No alarms

Actions Create volume

New EC2 Experience Tell us what you think

Successfully attached volume vol-0f8caa8e4b439146f to instance i-09b603873055f32e

Volumes (2)

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Availability Zone	Volume state	Alarm status
-	vol-030a3aa75fbfb03b	gp2	30 GiB	100	-	snap-03d182c...	2023/04/06 10:21 GMT+5...	ap-southeast-1a	In-use	No alarms
-	vol-0f8caa8e4b439146f	gp2	5 GiB	100	-	-	2023/04/06 11:13 GMT+5...	ap-southeast-1a	In-use	No alarms

Select a volume above

New EC2 Experience Tell us what you think

Successfully attached volume vol-0f8caa8e4b439146f to instance i-09b603873055f32e

Volumes (2)

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Availability Zone	Volume state	Alarm status
-	vol-030a3aa75fbfb03b	gp2	30 GiB	100	-	snap-03d182c...	2023/04/06 10:21 GMT+5...	ap-southeast-1a	In-use	No alarms
-	vol-0f8caa8e4b439146f	gp2	5 GiB	100	-	-	2023/04/06 11:13 GMT+5...	ap-southeast-1a	In-use	No alarms

Select a volume above

New EC2 Experience Tell us what you think

Successfully attached volume vol-0f8caa8e4b439146f to instance i-09b603873055f32e

Volumes (2)

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Availability Zone	Volume state	Alarm status
-	vol-030a3aa75fbfb03b	gp2	30 GiB	100	-	snap-03d182c...	2023/04/06 10:21 GMT+5...	ap-southeast-1a	In-use	No alarms
-	vol-0f8caa8e4b439146f	gp2	5 GiB	100	-	-	2023/04/06 11:13 GMT+5...	ap-southeast-1a	In-use	No alarms

Select a volume above

WindowsServer (1).rdp EC-2.pem EC-2.pem EC-2.pem EC-2.pem Show all

Screenshot of the AWS EC2 Management Console showing the successful launch of an instance.

Success
Successfully initiated launch of instance (i-0a8f64af985b6d9ed).

Next Steps

- Create billing and free tier usage alerts
- Connect to your instance
- Connect an RDS database
- Create EBS snapshot policy
- Manage detailed monitoring
- Create Load Balancer
- Create AWS budget
- Manage CloudWatch alarms

CloudShell Feedback Language

ec2-user@ip-172-31-20-110:~

```
Microsoft Windows [Version 10.0.22624.1537]
(c) Microsoft Corporation. All rights reserved.

Vis C:\linux>ssh -i EC-2.pem ec2-user@54.255.191.192
#_ _ _ _ _ Amazon Linux 2023
#_ _ _ _ _ https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-172-31-20-110 ~]$
```

Inbound security group rules successfully modified on security group (sg-03b0c88d0802ab481 | launch-wizard-2)

Details

sg-03b0c88d0802ab481 - launch-wizard-2

Details			
Security group name	Security group ID	Description	VPC ID
launch-wizard-2	sg-03b0c88d0802ab481	launch-wizard-2 created 2023-04-06T05:58:36.229Z	vpc-0340480eca8713d1
Owner	Inbound rules count	Outbound rules count	
660818258302	2 Permission entries	1 Permission entry	

Inbound rules (2)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sgr-0168e100a0x315b...	IPv4	SSH	TCP	22	0.0.0.0/0	-
-	sgr-0d4ec13e5f3b5f6e3	IPv4	HTTP	TCP	80	0.0.0.0/0	-

SACET S3 Management Console

Successfully created bucket "abdevilliers". To upload files and folders, or to configure additional bucket settings choose View details.

Amazon S3 > Buckets

Account snapshot

Buckets (5) info

Name	AWS Region	Access	Creation date
abdevilliers	Asia Pacific (Singapore) ap-southeast-1	Bucket and objects not public	April 11, 2023, 09:02:15 (UTC+05:30)
captainjcksparrow	Asia Pacific (Tokyo) ap-northeast-1	Objects can be public	April 10, 2023, 11:42:17 (UTC+05:30)
jagapraveen	Asia Pacific (Tokyo) ap-northeast-1	Objects can be public	April 10, 2023, 11:56:29 (UTC+05:30)
netturolex	Asia Pacific (Tokyo) ap-northeast-1	Objects can be public	April 10, 2023, 10:02:21 (UTC+05:30)
yogeshb	Asia Pacific (Tokyo) ap-northeast-1	Objects can be public	April 10, 2023, 11:40:16 (UTC+05:30)

CloudShell Feedback Language

Successfully created folder "Fida". Operation successfully completed.

Amazon S3 > Buckets > abdevilliers

abdevilliers Info

Objects (1)

Name	Type	Last modified	Size	Storage class
Fida/	Folder	-	-	-

CloudShell Feedback Language

S3ET x S3 Management Console x

s3.console.aws.amazon.com/x3/upload/abdevilliers?region=ap-southeast-1&prefix=Fida/

aws Services Search [Alt+S]

Global Jagapraveen G

Upload succeeded

View details below.

Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

Destination	Succeeded	Failed
s3://abdevilliers/Fida/	1 file, 167.4 KB (100.00%)	0 files, 0 B (0%)

Files and folders (1 Total, 167.4 KB)

Name	Folder	Type	Size	Status	Error
victory.jpg	-	image/jpeg	167.4 KB	Succeeded	-

S3ET x abdevilliers - S3 bucket x

s3.console.aws.amazon.com/x3/buckets/abdevilliers?region=ap-southeast-1&tab=permissions

aws Services Search [Alt+S]

Global Jagapraveen G

Successfully edited Block Public Access settings for this bucket.

Amazon S3 > Buckets > abdevilliers

abdevilliers [Info](#)

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit

Block all public access ⚠ OFF

► Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Edit Delete

No review to review. [View](#)

Screenshot of the AWS S3 console showing the permissions tab for the 'abdevilliers' bucket.

The top navigation bar shows the URL: s3.console.aws.amazon.com/v3/buckets/abdevilliers?region=ap-southeast-1&tab=permissions

The main content area displays the following information:

- Permissions overview:** Objects can be public.
- Block public access (bucket settings):** Block all public access is set to Off. A note states: "Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases." A link to "Learn more" is provided.
- Bucket policy:** No policy to display.

A second screenshot below shows the same bucket configuration after changing the public access setting to Public.

The top navigation bar shows the URL: s3.console.aws.amazon.com/v3/buckets/abdevilliers?region=ap-southeast-1&tab=permissions

The main content area displays the following information:

- Permissions overview:** Access is set to Public.
- Block public access (bucket settings):** Block all public access is set to Off. A note states: "Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases." A link to "Learn more" is provided.
- Bucket policy:** No policy to display.

Successfully edited access control list.

Amazon S3 > Buckets > abdevilliers

abdevilliers [Info](#)

Publicly accessible

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access Public

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit

Block all public access

Off

Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Edit Delete

CloudShell Feedback Language

SKCET abdevilliers - S3 bucket

CloudShell Feedback Language

Services Search [Alt+S]

Successfully edited public access

View details below.

Make public: status

The information below will no longer be available after you navigate away from this page.

Summary	
Source	s3://abdevilliers/Fida/
Result	Successfully edited 1 object, 167.4

S3ET abdevilliers - S3 bucket

Successfully edited public access

Make public: status

The information below will no longer be available after you navigate away from this page.

Summary

Source	Successfully edited public access	Failed to edit public access
s3://abdevilliers/Fida/	1 object, 167.4 KB	0 objects

Failed to edit public access

No objects failed to edit

Close

This screenshot shows the AWS S3 console interface. A success message at the top indicates that public access was successfully edited. Below it, a summary table shows one object successfully edited and zero objects failing. A separate section for failed edits shows zero objects. The configuration tab is also visible.

CloudShell Feedback Language

docs.aws.amazon.com IAM Management Console victory.jpg (1024x1280)

S3ET abdevilliers - S3 bucket

S3 Admins user group created

IAM User groups

User groups (1) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Create group

Group name	Users	Permissions	Creation time
S3 Admins	2 Loading	Defined	Now

View group

This screenshot shows the AWS IAM Management Console. It displays a success message for creating a new user group named "S3 Admins". The main view shows the "User groups" section with one group listed. The group has two users assigned and defined permissions. The creation time is noted as "Now".

S3ET doc.aws.amazon.com IAM Management Console IAM Management Console

Services Search [Alt+S] Global Jagapraveen G

Identity and Access Management (IAM)

Identity and Access Management (IAM) Search IAM Dashboard

Access management User groups Users Roles Policies Identity providers Account settings

Access reports Access analyzer Archive rules Analyzers Settings Credential report Organization activity Service control policies (SCPs)

Related consoles IAM Identity Center New

S3ET doc.aws.amazon.com IAM Management Console IAM Management Console

Services Search [Alt+S] Global Jagapraveen G

S3 Admin user group created. View group

User group deleted.

IAM > User groups

User groups (1) Info A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

Group name	Users	Permissions	Creation time
S3-Admin	0	Loading	Now

IAM > Users > Create user Step 1 Specify user details Step 2 Set permissions Step 3 Review and create Step 4 Retrieve password

User created successfully You can view and download the user's password and email instructions for signing in to the AWS Management Console. View user

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details Email sign-in instructions

Console sign-in URL https://660818258302.signin.aws.amazon.com/console

User name IAM1

Console password ***** Show

Download .csv file Return to users list

The screenshot shows two separate browser windows of the AWS IAM Management Console. The top window displays the 'User groups' page where a new group named 'S3-Admin' has been created. The bottom window shows the 'Create user' process, where a user named 'IAM1' has been successfully created, and the console provides sign-in details including a URL and a password.

S3ET X S3 Management Console X S3 Management Console X

s3.console.aws.amazon.com/v2/buckets?region=ap-southeast-1

aws Services Search [Alt+S]

Global Jagapraveen G

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Successfully created bucket "abdvishal". To upload files and folders, or to configure additional bucket settings choose View details.

Amazon S3 > Buckets

Account snapshot

Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (1) info

Buckets are containers for data stored in S3. Learn more

Find buckets by name

Name	AWS Region	Access	Creation date
abdvishal	Asia Pacific (Singapore) ap-southeast-1	Bucket and objects not public	April 11, 2023, 10:30:20 (UTC+05:30)

View details X

Copy ARN Empty Delete Create bucket

< 1 > ⌂

S3ET X abdvishal - S3 bucket X +

s3.console.aws.amazon.com/v2/buckets/abdvishal?region=ap-southeast-1&tab=objects

aws Services Search [Alt+S]

Global Jagapraveen G

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Successfully created folder "Kia". Operation successfully completed.

Amazon S3 > Buckets > abdvishal

abdvishal info

Objects Properties Permissions Metrics Management Access Points

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

Name	Type	Last modified	Size	Storage class
Kia/	Folder	-	-	-

Actions Copy S3 URI Copy URL Download Open Delete Create folder Upload

< 1 > ⌂

S3ET S3 Management Console

s3.console.aws.amazon.com/s3/upload/abdivishal?region=ap-southeast-1

aws Services Search [Alt+S]

Global Jagapraveen G

Upload succeeded

View details below.

Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

Destination	Succeeded	Failed
s3://abdivishal	1 file, 167.4 KB (100.00%)	0 files, 0 B (0%)

Files and folders (1 Total, 167.4 KB)

Name	Folder	Type	Size	Status	Error
victory.jpg	-	image/jpeg	167.4 KB	Succeeded	-

Close

Detailed description: This screenshot shows the AWS S3 Management Console interface. At the top, there's a header bar with the AWS logo, services dropdown, search bar, and user info. Below it, a green banner indicates a successful upload. The main area has a title 'Upload: status'. A note says the information will disappear if navigating away. Under 'Summary', it shows one file uploaded successfully to the root of 'abdivishal'. The 'Files and folders' section lists the single file 'victory.jpg' with its details: name, folder (empty), type (image/jpeg), size (167.4 KB), status (Succeeded), and error (empty). There are tabs for 'Files and folders' and 'Configuration'.

S3ET S3 Management Console

s3.console.aws.amazon.com/s3/upload/abdivishal?region=ap-southeast-1&prefix=Kia/

aws Services Search [Alt+S]

Global Jagapraveen G

Upload succeeded

View details below.

Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

Destination	Succeeded	Failed
s3://abdivishal/Kia/	1 file, 167.4 KB (100.00%)	0 files, 0 B (0%)

Files and folders (1 Total, 167.4 KB)

Name	Folder	Type	Size	Status	Error
victory.jpg	-	image/jpeg	167.4 KB	Succeeded	-

Close

Detailed description: This screenshot shows the AWS S3 Management Console interface, similar to the first one but with a specific prefix ('Kia') applied. The green banner indicates success. The summary shows one file uploaded to the 'Kia' prefix. The file listing table shows 'victory.jpg' with its details: name, folder ('Kia'), type (image/jpeg), size (167.4 KB), status (Succeeded), and error (empty). The tabs 'Files and folders' and 'Configuration' are present at the bottom.

Screenshot of the AWS S3 console showing the successful editing of Block Public Access settings for the 'abdvishal' bucket.

The 'Permissions' tab is selected. Under 'Access', it shows 'Objects can be public'. In the 'Block public access (bucket settings)' section, 'Block all public access' is set to 'OFF'. A note states: "Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases." A 'Learn more' link is provided.

The 'Bucket policy' section shows 'No policy to display.'

Screenshot of the AWS S3 console showing the successful editing of Object Ownership for the 'abdvishal' bucket.

The 'Permissions' tab is selected. Under 'Access', it shows 'Objects can be public'. In the 'Block public access (bucket settings)' section, 'Block all public access' is set to 'OFF'. A note states: "Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases." A 'Learn more' link is provided.

The 'Bucket policy' section shows 'No policy to display.'

S3ET abdышал - S3 bucket abdышал - S3 bucket https://abdышал.s3.ap-southeast-1.amazonaws.com/ [Alt+S]

aws Services Search [Alt+S]

Successfully edited public access

Make public: status

The information below will no longer be available after you navigate away from this page.

Summary

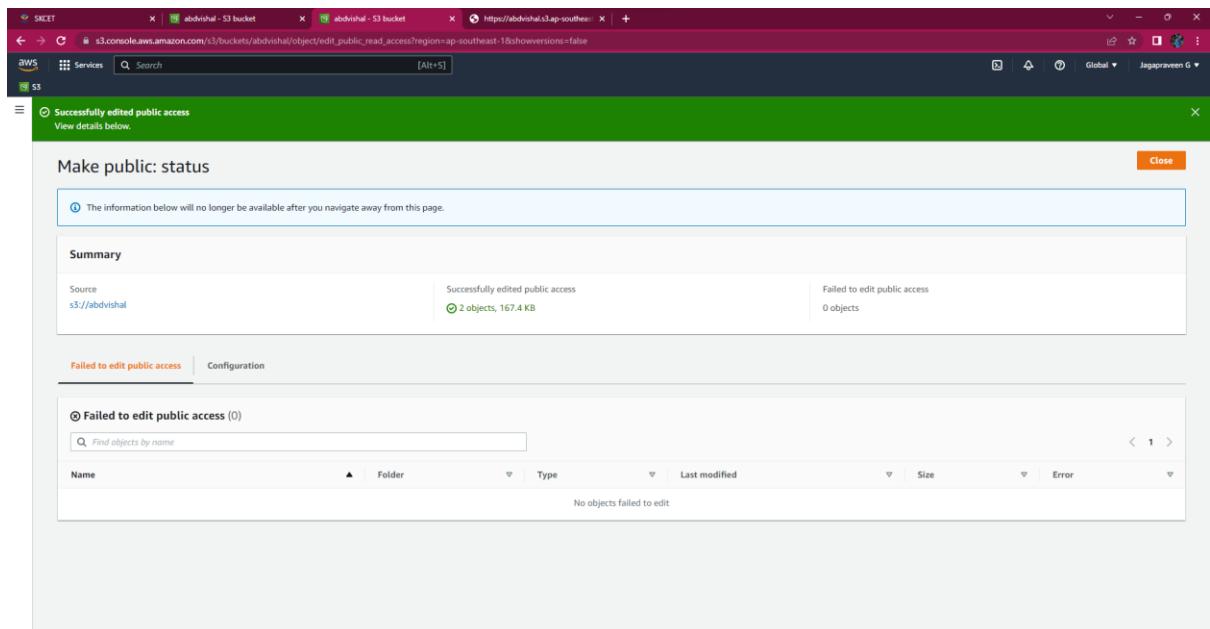
Source	Status	Details
s3://abdышал	Successfully edited public access	2 objects, 167.4 KB
	Failed to edit public access	0 objects

Failed to edit public access Configuration

Failed to edit public access (0)

Name	Folder	Type	Last modified	Size	Error
No objects failed to edit					

Close



S3ET abdышал - S3 bucket abdышал - S3 bucket AWS Policy Generator https://abdышал.s3.ap-southeast-1.amazonaws.com/ [Alt+S]

aws Services Search [Alt+S]

Successfully edited bucket policy.

Amazon S3 Buckets abdышал abdышал info

Permissions

Permissions overview

Block public access (bucket settings)

Block all public access

Edit

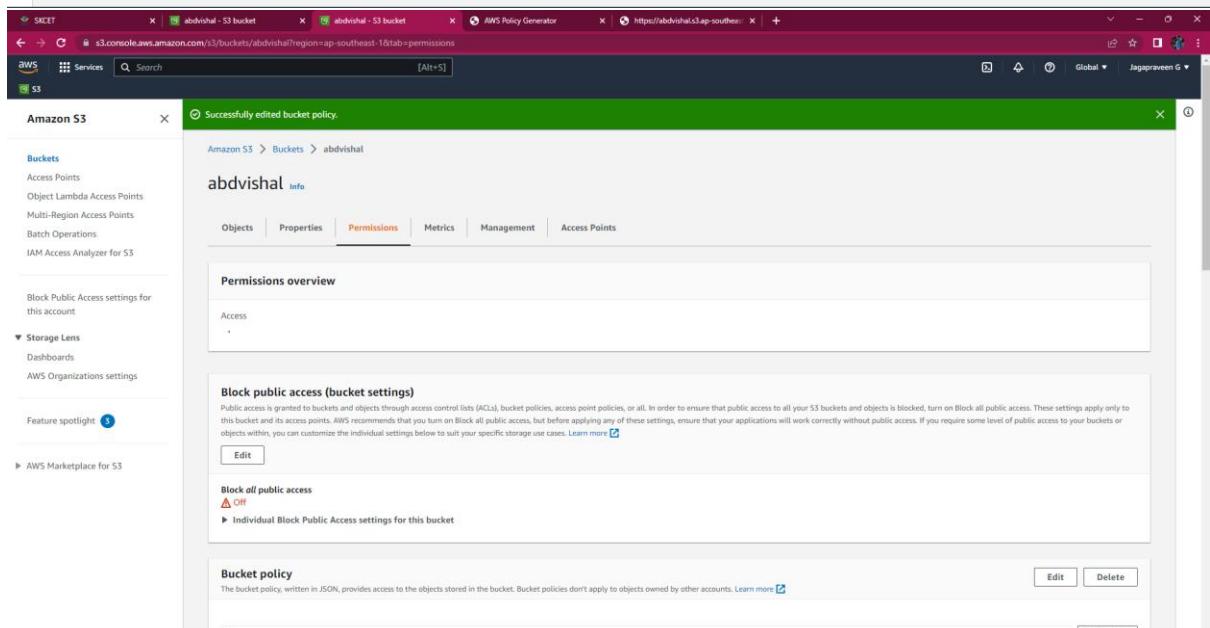
Off

Individual Block Public Access settings for this bucket

Bucket policy

Edit Delete

Cov



Successfully edited static website hosting.

Amazon S3 > Buckets > abdovichal

abdovichal info

Publicly accessible

Objects Properties Permissions Metrics Management Access Points

Bucket overview

AWS Region Asia Pacific (Singapore) ap-southeast-1	Amazon Resource Name (ARN) arnaws3:abdovichal	Creation date April 11, 2023, 10:30:20 (UTC+05:30)
---	--	---

Bucket Versioning

Versionsing is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more [Edit](#)

Bucket Versioning
Disabled

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more [Edit](#)

Tags (0)

You can use bucket tags to track storage costs and organize buckets. Learn more [Edit](#)

Successfully edited bucket policy.

Amazon S3 > Buckets > abdovichal

abdovichal info

Publicly accessible

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access
Public

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more [Edit](#)

Block all public access
Off

Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more [Edit Delete](#)

Screenshot of the AWS S3 Bucket Properties page for 'abdivishal' bucket.

Bucket Overview:

- AWS Region: Asia Pacific (Singapore) ap-southeast-1
- Amazon Resource Name (ARN): arnaws3:abdivishal
- Creation date: April 11, 2023, 10:30:20 (UTC+05:30)

Bucket Versioning:

Versionsing is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning Status: Enabled

Multi-factor authentication (MFA) delete: An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Tags (0): You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Upload status:

Summary:

Destination	Succeeded	Failed
s3://abdivishal/XYZ/	1 file, 12.0 B (100.0%)	0 files, 0 B (0%)

Files and folders (1 Total, 12.0 B):

Name	Folder	Type	Size	Status	Error
East.txt	-	text/plain	12.0 B	Succeeded	-

Screenshot of the AWS S3 Management Console showing the creation of a Lifecycle rule named "SweetBonda".

Step 1: Create Lifecycle Rule (Configuration Screen)

The "Days after object creation" field is set to 150.

Current version actions	Noncurrent versions actions
Day 0 • Objects uploaded	Day 0 • Objects become noncurrent
Day 30 • Objects move to Standard-IA	Day 30 • 99 newest noncurrent versions are retained • All other noncurrent versions move to Standard-IA
Day 100 • Objects move to Intelligent-Tiering	
Day 150 • Objects expire	

Step 2: Confirmation Message

The message states: "The lifecycle configuration was updated. Lifecycle rule "SweetBonda" was successfully added. It may take some time for the configuration to be updated. Press the refresh button if changes to the rule are not displayed."

Step 3: Lifecycle Configuration List

The "Lifecycle rules (1)" table shows the newly created rule:

Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions actions	Expired object delete markers	Incomplete multipart uploads
SweetBonda	Enabled	Entire bucket	Transition to Standard-IA, then Intelligent-Tiering, then expires	Transition to Standard-IA	-	-

The policy Napis has been created.

Policies (1066) Info

A policy is an object in AWS that defines permissions.

Policy name **Type** **Used as** **Description**

Napis	Customer managed	None	
AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read only access
AmazonGlacierReadOnlyAccess	AWS managed	None	Provides read only access
AWSMarketplaceFullAccess	AWS managed	None	Provides the ability to sub:
ClientVPNServiceRolePolicy	AWS managed	None	Policy to enable AWS Clie
AWSSSOAdministrator	AWS managed	None	Administrator access for S
AWSSloT1ClickReadOnlyAccess	AWS managed	None	Provides read only access
AutoScalingConsoleReadOnlyAccess	AWS managed	None	Provides read-only access
AmazonDMSRedshiftS3Role	AWS managed	None	Provides access to manag
AWSQuickSightListIAM	AWS managed	None	Allow QuickSight to list IAI
AWSHealthFullAccess	AWS managed	None	Allows full access to the A'
AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution

Policies attached to this user group

S3-Admin

Summary

User group name: S3-Admin Creation time: April 11, 2023, 10:18 (UTC+05:30) ARN: arn:aws:iam::660818258302:group/S3-Admin

Permissions

Permissions policies (2) Info

You can attach up to 10 managed policies.

Policy name **Type** **Description**

Napis	Customer managed	
AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the AW...

Failed to delete objects

For more information, see the Error column in the Failed to delete table below.

Delete objects: status

The information below will no longer be available after you navigate away from this page.

Summary

Source: s3://abdvishal	Successfully deleted: 0 objects	Failed to delete: 2 objects, 23.0 B
------------------------	---------------------------------	-------------------------------------

Meet - nym-vbyr-ou abdovichal - S3 bucket

s3.console.aws.amazon.com/v3/buckets/abdovichal/object/delete?region=ap-southeast-1&showversions=false

aws Services Search [Alt+S]

Failed to delete objects
For more information, see the Error column in the Failed to delete table below.

Delete objects: status

The information below will no longer be available after you navigate away from this page.

Summary

Source	Successfully deleted	Failed to delete
s3://abdovichal	0 objects	2 objects, 23.0 B

Failed to delete Configuration

Failed to delete (2 objects, 23.0 B)

Name	Folder	Type	Last modified	Size	Error
/	XYZ/	-	April 11, 2023, 11:07:07 (UTC+05:30)	0 B	Access denied
East.txt	XYZ/	txt	April 11, 2023, 11:09:32 (UTC+05:30)	23.0 B	Access denied

IAM Management Console IAM Management Console

us-east-1.console.aws.amazon.com/iamv2/home?region=ap-southeast-1#roles

aws Services Search [Alt+S]

Identity and Access Management (IAM)

Role doll created.

Identity > Roles

Roles (3) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Link...)	
doll	AWS Service: ec2	

Roles Anywhere info
Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads X.509 Standard Temporary credentials

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Manage

aws Services Search [Alt+S]

IAM S3 EC2

EC2 Instance created successfully

EC2 > Auto Scaling groups

Auto Scaling groups (1) Info

Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
EC2-Instance	Zarah Version Default	0	Updating capacity...	1	1	5	eu-west-2a, eu-west-2b

0 Auto Scaling groups selected

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

▼ Security

- Network ACLs
- Security groups

▼ DNS firewall

- Rule groups
- Domain lists

▼ Network Firewall

VPC dashboard X

EC2 Global View New

Filter by VPC: Select a VPC

▼ Virtual private cloud

Your VPCs New

- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs

VPC Management Console eu-west-2.console.aws.amazon.com/vpc/home?region=eu-west-2&VpcId=vpc-0e91235ede79e1468

aws Services Search [Alt+S]

You successfully created vpc-0e91235ede79e1468 / Zarah

VPC > Your VPCs > vpc-0e91235ede79e1468

vpc-0e91235ede79e1468 / Zarah

Details **Info**

VPC ID vpc-0e91235ede79e1468	State Available	DNS hostnames Disabled
Tenancy Default	DHCP option set dopt-01443f465758b99eb	Main route table rtb-0c1c5c1b3789ca710
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 807543533688

Resource map New CIDRs Flow logs Tags

Resource map Info

VPC Show details
Your AWS virtual network

Zarah

Introducing the VPC resource map
Solid lines represent relationships between resources in your VPC. Dotted lines represent relationships between resources in your VPC and other networks.

Subnets (0)
Subnets within this VPC

Route tables (1)
Route network traffic to resources

rtb-0c1c5c1b3789ca710

Network connections (0)
Connections to other networks

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

The screenshots show the AWS VPC console interface across three different browser tabs, illustrating the creation and attachment of a subnet and an internet gateway.

Screenshot 1: Subnet Creation

This screenshot shows the 'Subnets' page after creating a new subnet named 'Zarah-1'. The subnet details are as follows:

Name	Subnet ID	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
Zarah-1	subnet-08573d93bc556ad8d	vpc-0e91235ede79e1468 Zar...	10.0.0.0/16	-	65531

Screenshot 2: Internet Gateway Creation

This screenshot shows the 'Internet gateways' page after creating a new internet gateway named 'igw-0a9acb09fe5634391'. The gateway details are as follows:

Internet gateway ID	State	VPC ID	Owner
igw-0a9acb09fe5634391	Detached	-	807543533688

Screenshot 3: Internet Gateway Attachment

This screenshot shows the 'Internet gateways' page after attaching the internet gateway to a specific VPC. The gateway details are now updated to reflect the attachment:

Internet gateway ID	State	VPC ID	Owner
igw-0a9acb09fe5634391	Attached	vpc-0e91235ede79e1468 Zar...	807543533688

Route table rtb-06eb5b4723561216f | my-routes was created successfully.

VPC > Route tables > rtb-06eb5b4723561216f

rtb-06eb5b4723561216f / my-route

You can now check network connectivity with Reachability Analyzer

Actions

Details **Info**

Route table ID rtb-06eb5b4723561216f	Main No	Explicit subnet associations	Edge associations
VPC vpc-0e91235ede79e1468 Zarah	Owner ID 807543533688		

Routes **Subnet associations** **Edge associations** **Route propagation** **Tags**

Routes (1)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Edit routes

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Updated routes for rtb-06eb5b4723561216f / my-route successfully

VPC > Route tables > rtb-06eb5b4723561216f

rtb-06eb5b4723561216f / my-route

You can now check network connectivity with Reachability Analyzer

Actions

Details **Info**

Route table ID rtb-06eb5b4723561216f	Main No	Explicit subnet associations subnet-08573d93bc556ad8d / Zarah-1	Edge associations
VPC vpc-0e91235ede79e1468 Zarah	Owner ID 807543533688		

Routes **Subnet associations** **Edge associations** **Route propagation** **Tags**

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0a9acb09fe5634391	Active	No
10.0.0.0/16	local	Active	No

Edit routes

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Successfully created bucket "vishal17"

To upload files and folders, or to configure additional bucket settings choose View details.

Amazon S3

Buckets

- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- AWS Organizations settings

Feature spotlight:

AWS Marketplace for S3

View details

Amazon S3 > Buckets

Account snapshot

Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (1) Info

Buckets are containers for data stored in S3. Learn more

Name	AWS Region	Access	Creation date
vishal17	EU (London) eu-west-2	Objects can be public	April 19, 2023, 09:27:17 (UTC+05:30)

Create bucket

Copy ARN **Empty** **Delete**

Amazon S3

Successfully edited static website hosting.

Amazon S3 > Buckets > vishal17

vishal17 [Info](#)

Objects [Properties](#) Permissions Metrics Management Access Points

Bucket overview

AWS Region EU (London) eu-west-2	Amazon Resource Name (ARN) arn:aws:s3:::vishal17	Creation date April 19, 2023, 09:27:17 (UTC+05:30)
-------------------------------------	---	---

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

[Edit](#)

Bucket Versioning
Disabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Tags (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

[Edit](#)

Key	Value
-----	-------

Amazon S3

Successfully edited bucket policy.

Amazon S3 > Buckets > vishal17

vishal17 [Info](#)

Publicly accessible

Objects Properties [Permissions](#) Metrics Management Access Points

Permissions overview

Access Public

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

[Edit](#)

Block all public access
Off

[Individual Block Public Access settings for this bucket](#)

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

[Edit](#) [Delete](#)

Upload succeeded

View details below.

Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

Destination s3://vishal17	Succeeded 1 file, 105.0 B (100.00%)	Failed 0 files, 0 B (0%)
------------------------------	--	-----------------------------

[Files and folders](#) [Configuration](#)

Files and folders (1 Total, 105.0 B)

Name	Folder	Type	Size	Status	Error
index.html	-	text/html	105.0 B	Succeeded	-

aws Services Search [Alt+S] Global Kavya

Successfully edited public access

Make public: status

The information below will no longer be available after you navigate away from this page.

Summary

Source	Successfully edited public access	Failed to edit public access
s3://voishal17	1 object, 105.0 B	0 objects

Failed to edit public access Configuration

Failed to edit public access (0)

Name	Folder	Type	Last modified	Size	Error
No objects failed to edit					

aws Services Search [Alt+S] Global Kavya

Successfully created new distribution.

Do you have 30 seconds to share your experience? Help us improve CloudFront.

CloudFront > Distributions > E1YQVYUA4KU0FM

E1YQVYUA4KU0FM

General Origins Behaviors Error pages Geographic restrictions Invalidations Tags View metrics

Details

Distribution domain name	ARN	Last modified
d2lzpogwmrmxb.cloudfront.net	arn:aws:cloudfront:807543533688:distribution/E1YQVYUA4KU0FM	Deploying

Settings

Description	Alternate domain names	Standard logging
-	-	Off
Price class	-	Cookie logging
Use all edge locations (best performance)	-	Off
Supported HTTP versions	HTTP/2, HTTP/1.1, HTTP/1.0	Default root object
AWS WAF	-	-

Continuous deployment Create staging distribution

SKCET - Google Chrome skcet530.examly.io/test?id=f90363d8-bfe6-4ee5-801d-f6bc519f82d3105fd0ff-b110-4f00-aa07-18c55bfac900 Auto Submitted in 19 Apr 2023 | 04:35 PM 22:18 Submit Test

SKCET_CC2_Cloud_COD_Q3

Cloud Question (1)

Question No : 1 / 1

Cloud Question

Configure an AWS Application Load Balancer to distribute traffic to EC2 instances across multiple availability zones within a single region "Ohio".
Create an EC2 instance with the name tag "ec2instance1" in the "us-east-2a" availability zone.
Create another EC2 instance with the name tag "ec2instance2" in the "us-east-2b" availability zone.
Configure a http website in both the instances and allow http traffic (Port: 80) in the security group.
Create a Target group with the name "ec2targets".
Register the above created two instances in the "ec2targets" Target Group.
Create Loadbalancer with the name "ec2elb" by using "ec2targets" Target Group.

Note: While creating any AWS resources as per question either in Terraform or console, if you see any error saying that the resource "already exists" then kindly delete the existing resource and create your new resource. If VPC limit exceeds also, then kindly delete the existing VPC and create your new VPC.

Click the below AWS account link and copy paste the given User Name and Password to start

AWS Account URL:

AWS User Name:

AWS Password:

Run Test Case Submit Cloud

Answered 0/1 Bookmarked 0/1 Skipped 0/1 Not Viewed 0/1 Saved in Server 0/1 View More



SRI KRISHNA COLLEGE OF ENGINEERING AND TECHNOLOGY
(An Autonomous Institution and affiliated to Anna University, Chennai)
Kuniamuthur, Coimbatore - 641 008



OFFICE OF THE CONTROLLER OF EXAMINATIONS
END SEMESTER EXAMINATIONS - APR/MAY 2023 (REGULAR)

PROGRAMME : B.TECH ARTIFICIAL INTELLIGENCE AND DATA SCIENCE
SEMESTER: IV

SESSION: FN - 09.30 AM TO 12.30 PM

S.NO	DATE	SESSION	COURSE CODE	COURSE NAME
1	29-May-2023	FN	21MA404	RANDOM VARIABLES AND STATISTICS
2	31-May-2023	FN	21AD401	FUNDAMENTALS OF OPERATING SYSTEMS
3	02-Jun-2023	FN	21AD402	DATA WAREHOUSING AND MINING
4	05-Jun-2023	FN	21CS402	WEB FRAMEWORKS
5	07-Jun-2023	FN	21IT402	SOFTWARE TESTING USING SELENIUM
6	09-Jun-2023	FN	21AD403	CLOUD COMPUTING

CONTROLLER OF EXAMINATIONS

aws Services Search [Alt+S] Ohio Kavya

EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-040dfb690421c3cf9)

▶ Launch log

Next Steps

Q. What would you like to do next with this instance, for example "create alarm" or "create backup"?

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

[Create billing alerts](#)

Connect to your instance

Once your instance is running, log into it from your local computer.

[Connect to instance](#)

[Learn more](#)

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

[Connect an RDS database](#)

[Create a new RDS database](#) [Learn more](#)

Create EBS snapshot policy

Create a policy that automates the creation, retention, and deletion of EBS snapshots

[Create EBS snapshot policy](#)

Manage detailed monitoring

Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.

[Manage detailed monitoring](#)

Create Load Balancer

Create a application, network gateway or classic Elastic Load Balancer

[Create Load Balancer](#)

Create AWS budget

AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.

[Create AWS budget](#)

Manage CloudWatch alarms

Create or update Amazon CloudWatch alarms for the instance.

[Manage CloudWatch alarms](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences Ohio Kavya

EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-00309d04ef929d232)

▶ Launch log

Next Steps

Q. What would you like to do next with this instance, for example "create alarm" or "create backup"?

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

[Create billing alerts](#)

Connect to your instance

Once your instance is running, log into it from your local computer.

[Connect to instance](#)

[Learn more](#)

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

[Connect an RDS database](#)

[Create a new RDS database](#) [Learn more](#)

Create EBS snapshot policy

Create a policy that automates the creation, retention, and deletion of EBS snapshots

[Create EBS snapshot policy](#)

Manage detailed monitoring

Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.

[Manage detailed monitoring](#)

Create Load Balancer

Create a application, network gateway or classic Elastic Load Balancer

[Create Load Balancer](#)

Create AWS budget

AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.

[Create AWS budget](#)

Manage CloudWatch alarms

Create or update Amazon CloudWatch alarms for the instance.

[Manage CloudWatch alarms](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences Ohio Kavya

EC2 > Target groups

Successfully created target group: ec2Targets

EC2 > Target groups

Target groups (1) Info

Search or filter target groups

Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
ec2Targets	arn:aws:elasticloadbalanc...	80	HTTP	Instance	None associated	vpc-0514ffea6a4ce8411

0 target groups selected

Select a target group above.

New EC Experience Tell us what you think

EC2 Dashboard EC2 Global View Events Tags Limits Instances Instances Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservations Images AMIs AMI Catalog Elastic Block Store Volumes Snapshots Lifecycle Manager Network & Security Security Groups Elastic IPs

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences Ohio Kavya

